UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ACW FLEX PACK LLC,	)	
	)	
Plaintiff,	)	Case No. 22-cv-6858
	)	
v.	)	Hon. Steven C. Seeger
	)	
CHRISTOPHER WROBEL and	)	
THOMAS RYAN,	)	
	)	
Defendants.	)	
	)	

MEMORANDUM OPINION AND ORDER

Plaintiff ACW Flex Pack LLC sent a few people packing. First, the company let go its CEO, Defendant Christopher Wrobel, for underperformance. And then, about 18 months later, the company cut the cord with its IT director, Defendant Thomas Ryan.

There is nothing especially noteworthy about changing personnel, especially in the senior leadership ranks. Letting people go is a bread-and-butter part of any business. But here, the company discovered misconduct that was anything but business as usual.

During Ryan's last month as IT director, ACW learned that he was deleting company documents, including Wrobel's old emails. The deletion of files was just the tip of the iceberg. A forensic analysis showed that Wrobel and Ryan set up an email account for a fake employee, and gave that account access to everything on the company's cloud computing system. And then, Wrobel used that account to rummage through company files, long after his departure. Worse yet, Ryan never deleted Wrobel's personal access after the company let him go.

ACW responded by suing Wrobel and Ryan about the unauthorized access to its computer files. The complaint includes seven claims under federal and state law. Defendants, in turn, moved to dismiss four of the seven claims. Specifically, they moved to dismiss the claims under two federal statutes, the Computer Fraud and Abuse Act and the Stored Communications Act. Defendants also moved to dismiss the state law claims for conversion and civil conspiracy.

For the following reasons, the motion to dismiss is denied in part and granted in part.

Background

At the motion-to-dismiss stage, the Court must accept as true the complaint's well-pleaded allegations. *See Lett v. City of Chicago*, 946 F.3d 398, 399 (7th Cir. 2020). The Court "offer[s] no opinion on the ultimate merits because further development of the record may cast the facts in a light different from the complaint." *Savory v. Cannon*, 947 F.3d 409, 412 (7th Cir. 2020).

This case is about a CEO and an IT director who covertly accessed a company's documents and emails stored in the cloud.

Plaintiff ACW Flex Pack LLC owns several companies that produce "specialty pouches and related products for the growing flexible packaging market." *See* Cplt., at ¶ 10 (Dckt. No. 1). The packaging is useful for household products including "frozen foods, coffee, detergents and cleaning products, yogurt and baby foods, and snack products." *Id.* at ¶ 13.

In June 2018, Defendant Christopher Wrobel became ACW's CEO. *Id.* at ¶ 15. As the CEO, Wrobel had access to ACW's confidential information. "Wrobel had direct access to key confidential informational for each of the ACW subsidiary companies, including sourcing information, manufacturing costs for various products, manufacturing techniques, customer lists, and customer pricing." *Id.*

Soon after he became the CEO, Wrobel hired All Covered, a third-party IT-services firm to manage ACW's IT needs. *Id.* at ¶ 26. Defendant Thomas Ryan was an employee of All

Covered. *Id.* at ¶¶ 25–26. Wrobel had known Ryan since childhood. *Id.* at ¶ 24. They were childhood buddies. *Id.*

In February 2020, Ryan's relationship with ACW changed. Instead of supplying IT services in his role as an All Covered employee, Ryan "became a consultant for ACW and entered into a direct relationship with the company." *Id.* at ¶ 27. Ryan and one of ACW's companies entered into an independent contractor agreement. *Id.* at ¶ 28. Under the agreement, "Ryan agreed to provide data management and coordinate information systems for ACW." *Id.* at ¶ 29.

Ryan's role was "to operate as the head of technology and information services for ACW." *Id.* at ¶ 30. To do the job, he "was provided with global administrative access to ACW's computer and data systems." *Id.*

ACW used Microsoft Office 365 cloud services. *Id.* at ¶ 31. The services included OneDrive, SharePoint, and Exchange. *Id.* "Microsoft 365 can house and manage documents created and stored for an individual (OneDrive), documents created and stored for access and collaboration among groups of ACW employees (SharePoint), and e-mail (Exchange)." *Id.* at ¶ 40. That is, ACW used Microsoft's document storage and email services, which could be accessed remotely through the cloud.

Through Microsoft 365's cloud services, "ACW employees have the ability to access workplace data both while on ACW premises as well as remotely." *Id.* at ¶ 31. To get access to ACW's Microsoft 365 services, ACW provided user accounts and permissions through Microsoft. *Id.* ACW employees were "issued their own email account and [were] required to create a username and password to access ACW's computer system." *Id.* at ¶ 53.

Ryan oversaw and administered access to ACW's Microsoft 365 system. *Id.* at ¶ 32. After he became an independent contractor, "Ryan was one of a very small number of individuals with global administrative access to ACW's system." *Id.* From an IT standpoint, he held the keys to the kingdom.

Wrobel also relied on Ryan for more than IT services. He "sought assistance from Ryan on product pricing," and "would include [Ryan] in executive meetings and strategy sessions." *Id.* at ¶ 33. During early 2021, "Wrobel provided Ryan significant pricing responsibilities as well as preparing monthly [inventory valuation] evaluations." *Id.*

Wrobel's time as ACW's CEO was relatively short lived. "After more than two years of non-performance, Wrobel was informed he would be replaced as the CEO on March 31, 2021." *Id.* at ¶ 17. Scott Myers stepped in as the new CEO. *Id.*

As Myers transitioned to the CEO role, he "was given access to Wrobel's email files to ensure he could maintain company projects and relationships developed on behalf of ACW by being able to respond to newly arrived emails and to utilize Wrobel's old emails for reference." *Id.* at ¶ 18.

At the same time, Myers eliminated Wrobel's access to ACW's computer systems. *Id.* at ¶ 19. Or so he thought. Specifically, Myers instructed Ryan to remove Wrobel's access to ACW's networks. *Id.* Wrobel also was "asked to return any and all ACW company property and information in his possession." *Id.* at ¶ 20.

Wrobel's departure from ACW turned out to be bad news for Ryan, too. Shortly after Myers took over as CEO, he transferred responsibility for product pricing from Ryan to a different employee. *Id.* at ¶ 34.

In September 2022, about a year and a half after Wrobel's departure, Myers ended Ryan's contract with ACW and hired a new head of IT. *Id.* Myers "explicitly instructed Ryan not to delete, change or take information from ACW's computer systems." *Id.* at ¶ 36. Ryan said that he wouldn't do so. *Id.*

Ryan's termination called for a soft landing. He would be paid through October 14, 2022, but until this end date "he would only need to be available to assist in transition or answer questions because a newly-hired employee would be taking over responsibilities for ACW's IT management." *Id.* at ¶ 35.

Ryan never made it to his scheduled end date. On October 11, 2022, "employees at ACW discovered that Ryan had taken actions to eliminate Myers' access to Wrobel's ACW email." *Id.* at ¶ 37. "Specifically, ACW discovered that Ryan deleted Wrobel's email from ACW's system which included his historical email files." *Id.* So, Ryan prevented the new CEO (Myers) from getting access to the emails of the old CEO (Wrobel).

Needless to say, it didn't sit well with ACW that the head of IT was deleting files on his way out the door. After it learned that Ryan was deleting Wrobel's emails, it "immediately cut off Ryan's access to their computer systems." *Id.* at ¶ 39.

ACW also conducted a third-party forensic review of its systems. *Id.* at ¶ 62. The analysis revealed that both Ryan and Wrobel improperly accessed ACW's computer systems.

For starters, back in January 2020, Ryan and Wrobel set up an ACW email account for a user named Jay Atwater. *Id.* at ¶ 64. Ryan used his personal email account to send Wrobel an email with instructions on creating an account for Atwater. *Id.* at ¶ 65.

There was one problem. No employee named Jay Atwater ever worked at ACW. *Id.* at ¶ 64. Ryan and Wrobel created an email account for a fake person.

But that fake person had very real access to ACW's systems. Ryan gave Atwater's account "Global Administration Rights to the ACW systems that would allow the account to have access to all system locations as well as the email of everyone at ACW." *Id.* at ¶ 66.

The Atwater account also had some longevity. Ryan updated the account in April 2022, more than two years after it was created. *Id.* Ryan ultimately deleted the Atwater account in September 2022, after learning that he was being terminated. *Id.* at ¶ 68.

Creating the Atwater account was not Ryan's only improper access to ACW's systems. Ryan also facilitated Wrobel's access to ACW's systems after ACW fired Wrobel. Despite being instructed in April 2021 to delete Wrobel's access to ACW's computer systems, Ryan never did so. *Id.* at ¶ 19. Wrobel then "accessed multiple ACW services after his departure from ACW when he took advantage of the unauthorized access to ACW's system." *Id.* at ¶ 70.

Forensic analysis revealed that from July to September 2022, the user "chris.wrobel@capadllc.com" logged in to ACW's system more than 100 times on 29 different days. *Id.* at ¶ 72. While logged in, Wrobel's account "accessed documents stored on ACW's SharePoint system that contain ACW's confidential information and Trade Secrets." *Id.* at ¶ 73. Though the forensic analysis goes back to only July 2022, ACW alleges "upon information and belief" that Wrobel likely accessed ACW's systems numerous times before then. *Id.* at ¶ 74.

Forensic analysis also showed that Ryan improperly accessed ACW's network after he learned that he was being terminated. *Id.* at ¶¶ 75–76. Ryan deleted the Atwater account before his last day. *Id.* at ¶¶ 68, 77. Ryan also deleted the user "chris.wrobel@capadllc.com" and "removed . . . Wrobel's personal domain (capadllc.com) and email from the ACW [Microsoft] 365 tenant and deleted Wrobel's ACW email box." *Id.* at ¶¶ 78–79. Apparently, he spent his final days at ACW trying to cover his tracks.

Ryan also "downloaded extensive ACW information." *Id.* at ¶ 80. "The information downloaded from both ACW's OneDrive and SharePoint locations contained ACW Trade Secrets including customer lists; archived pricing tool records with customer quotes; other pricing documents; order entries; and project RFPs." *Id.* In total, Ryan downloaded 11,030 files from ACW's system. *Id.*

Ryan did not merely download files – he also deleted them. "Almost immediately after downloading thousands of ACW's files containing proprietary information, Ryan deleted thousands of files, folders, and items from ACW's OneDrive and SharePoint system." *Id.* at ¶ 81. The deleted files "contained ACW's pricing lists, financial information, and other confidential and ACW Trade Secret documents." *Id.*; *see also id.* at ¶ 82. After discovering that Ryan had deleted the files, ACW's new IT personnel restored the deleted files to the system. *Id.* at ¶ 83.

ACW alleges that Wrobel's and Ryan's access of the files was unauthorized. "At no point did ACW authorize either Wrobel or Ryan to access, transfer, take, or delete any of ACW's Trade Secrets and confidential information or use it for any purpose outside of their respective duties for ACW." *Id.* at ¶ 84. ACW believes that "Wrobel and Ryan knowingly and improperly accessed ACW proprietary information and Trade Secrets." *Id.* at ¶ 86.

On November 4, 2022, ACW sent both Wrobel and Ryan cease-and-desist letters, demanding that they stop accessing ACW's data and that they return any data taken from ACW. *Id.* at ¶ 88. To date, none of ACW's data or information has been returned. *Id.* at ¶ 89.

So, ACW sued Wrobel and Ryan. *See* Cplt. (Dckt. No. 1). The complaint has seven counts. Count I alleges that Wrobel and Ryan violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*, for their unauthorized access of ACW's network. *Id.* at

¶¶ 90–101. Count II alleges that Defendants violated the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*, by accessing ACW's network without authorization. *Id.* at ¶¶ 102–11. Count III alleges a violation of the Defend Trade Secrets Act. *Id.* at ¶¶ 112–23. Count IV is a claim under the Illinois Trade Secrets Act. *Id.* at ¶¶ 124–35. Count V alleges that Ryan breached his independent contractor agreement. *Id.* at ¶¶ 136–45. Count VI alleges that Defendants converted ACW's property when they took its confidential information and trade secrets. *Id.* at ¶¶ 146–50. And Count VII alleges that Defendants committed civil conspiracy when misappropriating ACW's confidential information and trade secrets. *Id.* at ¶¶ 151–58.

Defendants moved to dismiss only four of the seven counts. *See* Defs.' Mtn. to Dismiss (Dckt. No. 10). They moved to dismiss the claims under the first two federal statutes, meaning the Computer Fraud and Abuse Act (Count I) and the Stored Communications Act (Count II). They also moved to dismiss the state law claims for conversion (Count VI) and civil conspiracy (Count VII). *Id.*

Legal Standard

A motion to dismiss under Rule 12(b)(6) challenges the sufficiency of the complaint, not its merits. *See* Fed. R. Civ. P. 12(b)(6); *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). In considering a Rule 12(b)(6) motion to dismiss, the Court accepts as true all well-pleaded facts in the complaint and draws all reasonable inferences from those facts in the plaintiff's favor. *See AnchorBank, FSB v. Hofer*, 649 F.3d 610, 614 (7th Cir. 2011). To survive a Rule 12(b)(6) motion, the complaint must provide the defendant with fair notice of the basis for the claim, and it must be facially plausible. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678.

Analysis

The Court begins by considering ACW's claims under two federal statutes, the Computer Fraud and Abuse Act and the Stored Communications Act. Then, the Court turns to ACW's state law claims for conversion and civil conspiracy. The punchline is that the Court denies the motion to dismiss the federal claims, but grants the motion to dismiss the state law claims.

I. Computer Fraud and Abuse Act Claim (Count I)

The Computer Fraud and Abuse Act "is primarily a criminal anti-hacking statute." *Fidlar Techs. v. LPS Real Est. Data Sols., Inc.*, 810 F.3d 1075, 1079 (7th Cir. 2016). After all, the statute is in Title 18 of the U.S. Code, which primarily lists federal crimes. *See* 18 U.S.C. § 1030 *et seq*. But the statute also creates a private right of action "which allows persons suffering 'damage' or 'loss' from CFAA violations to sue for money damages and equitable relief." *Van Buren v. United States*, 141 S. Ct. 1648, 1657 (2021) (quoting 18 U.S.C. § 1030(g)).

ACW sued under section 1030(g) and alleged that Wrobel and Ryan violated two subsections of the Consumer Fraud and Abuse Act, subjecting them to civil liability.

First, ACW alleged that Defendants violated section 1030(a)(2). *See* Cplt., at ¶¶ 92, 94 (Dckt. No. 1). Section 1030(a)(2) creates liability for anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." *See* 18 U.S.C. § 1030(a)(2)(C). "The elements of a section 1030(a)(2) violation thus include (1) intentional access of a computer, (2) without or in excess of authorization, (3) whereby the defendant obtains information from the protected computer." *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 766 (N.D. Ill. 2009).

Second, ACW alleged that Defendants violated section 1030(a)(4). *See* Cplt., at ¶ 99 (Dckt. No. 1). Section 1030(a)(4) prohibits fraud by computer hacking. The Act creates liability for anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." *See* 18 U.S.C. § 1030(a)(4).

Defendants offer a single reason why ACW's claim under the Consumer Fraud and Abuse Act (including both section 1030(a)(2) and section 1030(a)(4)) should be dismissed.[1] *See* Defs.' Mtn. to Dismiss, at 2–3 (Dckt. No. 10). They note that the "CFAA requires the alleged wrongdoer to access a 'computer' or 'protected computer.'" *Id.* at 3. Defendants contend that ACW has not alleged that they accessed a computer because the complaint alleges that they accessed ACW's *cloud system*. *Id.*

"While the Plaintiff goes to great lengths to describe the cloud-based system of data storage utilized by ACW (which might be characterized as a facility), the Plaintiff fails to allege with any degree of specificity how the defendants accessed any computer owned by ACW as it is defined in the Act." *Id.*

[1] Defendant did not make any argument for dismissal of the Computer Fraud and Abuse Act claim based on the Supreme Court's recent decision in *Van Buren v. United States*, 141 S. Ct. 1648 (2021). *See* Defs.' Mtn. to Dismiss, at 2–3 (Dckt. No. 10). *Van Buren* held that whether an individual accesses a computer "without authorization" or "exceeds authorized access" depends on "a gates-up-or-down inquiry – one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Van Buren*, 141 S. Ct. at 1658–59. The user's purpose for accessing the information is irrelevant. *Id.* at 1655. Instead, "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders, or databases – that are off limits to him." *Id.* at 1662. So, if Ryan or Wrobel had rightful access to ACW's files for some purpose, but accessed the files for an impermissible purpose, then ACW does not have a claim under the Computer Fraud and Abuse Act.

In Defendants' view, ACW alleges only that they accessed its cloud system. It does not allege that they accessed a physical computer that it owned. So, Defendants' argument depends on the meaning of "computer" in the Act.

The Act includes definitions of key terms, which control the meaning of the statute. "When 'a statute includes an explicit definition' of a term, 'we must follow that definition, even if it varies from a term's ordinary meaning.'" *Van Buren*, 141 S. Ct. at 1657 (quoting *Tanzin v. Tanvir*, 141 S. Ct. 486, 490 (2020)).

The Consumer Fraud and Abuse Act uses an expansive, all-inclusive definition of the term "computer." Under the statute, "the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, *and includes any data storage facility or communications facility directly related to or operating in conjunction with such device*." *See* 18 U.S.C. § 1030(e)(1) (emphasis added).

So, when the Consumer Fraud and Abuse Act mentions "computers," the statute is referring not just to the hardware that you might associate with the term "computer" in everyday conversation. Instead, the term "computer" also "includes a 'communications facility directly related to or operating in conjunction with' a computer." *United States v. Featherly,* 846 F.3d 237, 240 (7th Cir. 2017) (per curiam) (quoting 18 U.S.C. § 1030(e)(1)).

For example, a modem – a device that allows access to the Internet – is a "communications facility" under section 1030(e)(1) because "it's a device that operates in conjunction with a computer to enable communication with others over the Internet." *Id.* So, under the Consumer Fraud and Abuse Act, a modem meets the definition of "computer." *Id.*

The Seventh Circuit has noted that the Consumer Fraud and Abuse Act gives a "very, very broad definition" of "computer." *United States v. Shamsud-Din*, 580 F. App'x 468, 472 (7th Cir. 2014). The Act's definition of computer is so broad that it "could encompass a cell phone." *Id.* (citing *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005)).

The Act also defines "protected computer." *See* 18 U.S.C. § 1030(e)(2). Once again, the term is expansive. It "cover[s] any information from any computer 'used in or affecting interstate or foreign commerce or communication.'" *Van Buren*, 141 S. Ct. at 1652 (quoting 18 U.S.C. § 1030(e)(2)(B)). So, a "protected computer" is any computer as defined in section 1030(e)(1) used in or affecting interstate or foreign commerce or communication.

Defendants argue that by accessing ACW's cloud-based network, they were not accessing a "computer" within the meaning of the Act. Not so. ACW has plausibly alleged that by accessing the data on Microsoft's 365 cloud services, Defendants accessed a "computer" as defined by the Consumer Fraud and Abuse Act.

For starters, the "cloud" is a metaphor. It does not refer to meteorology. Instead, in this context, "the cloud" refers to "cloud *computing*," which has computing right in the name. "Cloud computing" typically means "the practice of storing regularly used computer data on multiple servers that can be accessed through the Internet."[2]

The Supreme Court has recognized this meaning of the term. "Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 573 U.S. 373, 397 (2014).

So, data stored in the cloud is actually stored on a physical server, somewhere in the world. And what's a server? A server is a computer.

[2] *See Cloud Computing*, Merriam-Webster Online, https://www.merriam-webster.com/dictionary/cloud%20computing (last visited July 24, 2023).

Servers fit within the plain language of the Act. A server is a computer because it is a "data processing device." *See* 18 U.S.C. § 1030(e)(1). That's the whole point of a server – processing and retaining data. The Act's definition of a computer also "includes a 'communications facility directly related to or operating in conjunction with' a computer." *Featherly*, 846 F.3d at 240 (quoting 18 U.S.C. § 1030(e)(1)). By its nature, a server operates in conjunction with other computers because it "manage[s] network resources and provide[s] data to other computers." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195 (9th Cir. 2022).

That statutory definition fits with ordinary usage. The dictionary defines "server" as "*a computer* in a network that is used to provide services (such as access to files or shared peripherals or the routing of email) to other computers in the network."[3]

Both the Ninth and Eleventh Circuits have squarely held that servers are "computers" within the meaning of the Consumer Fraud and Abuse Act. The Act's definition of "computer" "include[s] servers, *computers that manage network resources and provide data to other computers*." *hiQ Labs*, 31 F.4th at 1195 (emphasis added). Servers "clearly qualify as 'computer[s]'" under the Act. *SkyHop Techs., Inc. v. Narra*, 58 F.4th 1211, 1227 (11th Cir. 2023) (alteration in original) (quoting *hiQ Labs*, 31 F.4th at 1195).

So, if accessing data in the cloud requires the user to access a server, and if a server is a computer, then by accessing ACW's data on Microsoft's cloud, Defendants accessed a computer. After all, "[m]any websites, services, and databases . . . provide 'information' from 'protected computer[s]'" and fall within the Act's scope. *Van Buren*, 141 S. Ct. at 1661 (third alteration in original) (quoting 18 U.S.C. § 1030(a)(2)(C)).

[3] *See Server*, Merriam-Webster Online, https://www.merriam-webster.com/dictionary/server (last visited July 24, 2023) (emphasis added).

Defendants seem to argue that they did not violate the Consumer Fraud and Abuse Act if ACW did not own the computer. *See* Defs.' Mtn. to Dismiss, at 3 (Dckt. No. 10) ("[T]he Plaintiff fails to allege with any degree of specificity how the defendants accessed any computer *owned by* ACW as it is defined in the Act.") (emphasis added).

Ownership does not matter. "It makes no difference that [ACW] does not own the servers ([presumably Microsoft] does). Those servers are cloud-based and permit users to access their data and information from anywhere via the internet." *SkyHop Techs.*, 58 F.4th at 1127.

The Act does not require that the plaintiff own the computer. It prohibits "intentionally accesses a computer without authorization or exceed[ing] authorized access." *See* 18 U.S.C. § 1030(a)(2); *see also id.* § 1030(a)(4). Nowhere does the Act create an ownership requirement. And as a practical matter, companies often have rights to things that they do not own (*e.g.*, leasing office space).

In their reply brief, Defendants latch on to the word "device" in the Act's definition of "computer." They argue that a computer must be a "device" or "any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* Defs.' Reply, at 2 (Dckt. No. 14) (quoting 18 U.S.C. § 1030(e)(1)). In Defendants' view, a device is "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function." *Id.* (quotation marks omitted). And a computer being a device "is contrary to the cloud-based system at issue." *Id.*

Even assuming that a computer must be a device, ACW's cloud-based system would fit the bill. Again, storing data in "the cloud" does not mean that ACW's data is stored as molecules in the atmosphere. The cloud is a metaphor for a server that stores data. And a server is a device under Defendants' definition. It is a physical piece of equipment designed to serve a special purpose or perform a special function.

In sum, the Court denies Defendants' motion to dismiss ACW's claim under the Computer Fraud and Abuse Act. By alleging that Defendants accessed data stored on Microsoft 365's cloud-computing system, ACW has plausibly alleged that Defendants accessed a computer within the meaning of the Act.

II. Stored Communications Act Claim (Count II)

The second claim falls under a similar federal statute, the Stored Communications Act. Once again, the complaint passes muster.

"The Stored Communications Act prohibits unauthorized access to communications in electronic storage." *Uebelacker v. Rock Energy Coop.*, 54 F.4th 1008, 1010 (7th Cir. 2022). "Congress passed the SCA to protect privacy interests in personal and proprietary information." *Int'l Bhd. of Elec. Workers, Loc. 134 v. Cunningham*, 2013 WL 1828932, at *2 (N.D. Ill. 2013). Like the Computer Fraud and Abuse Act, the Stored Communications Act is primarily a criminal statute that also creates a private right of action. *See* 18 U.S.C. §§ 2701(b), 2707. Any person "aggrieved by any violation" of the statute may sue. *Id.* § 2707(a).

The Stored Communications Act creates liability for anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." *Id.* § 2701(a)(1)–(2). That is, "[t]he SCA provides a private cause of action for unauthorized, intentional access to communications held in electronic storage." *Joseph v. Carnes*, 13508 F. Supp. 3d 613, 616 (N.D. Ill. 2015) (quoting *Maremont v. Susan Fredman Design Grp., Ltd.*, 2014 WL 812401, at *6 (N.D. Ill. 2014)).

The Act focuses on access – not misuse. The SCA "prohibits only unauthorized access and not the misappropriation or disclosure of information." *Lane v. Brocq*, 2016 WL 1271051, at *6 (N.D. Ill. 2016) (quotation marks omitted); *see also BI3 v. Hamor*, 2009 WL 2192801, at *3 (N.D. Ill. 2009) (noting that the SCA "prohibits unauthorized access to the facility, and would not protect the plaintiffs against misuse of information or property if access to the facility was authorized").

Like the Consumer Fraud and Abuse Act, the Stored Communications Act includes a set of defined terms. The Act defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *See* 18 U.S.C. § 2510(15); *see also id.* § 2711(1) (making the definitions in section 2510 applicable to the Stored Communications Act).

"Electronic communication" is defined broadly. It "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id.* § 2510(12). "The plain language of this definition encompasses email." *Hately v. Watts*, 917 F.3d 770, 785 (4th Cir. 2019).

Applying these definitions, "courts have interpreted the SCA to target providers of wire or electronic communications services, 'such as telephone companies, Internet or e-mail service providers, and bulletin board services.'" *Loughnane v. Zukowski, Rogers, Flood & McArdle*, 2021 WL 1057278, at *3 (N.D. Ill. 2021) (Lee, J.) (quoting *Garcia v. City of Laredo*, 702 F.3d 788, 792 (5th Cir. 2012)). "A defendant violates the SCA when he intentionally accesses his co-workers' email accounts without authorization." *Bloomington-Normal Seating Co. v. Albritton*, 2009 WL 1329123, at *4 (C.D. Ill. 2009).

For example, the Fourth Circuit has held "that companies such as Microsoft and Google function as an electronic communication services [under the SCA] when they provide email services through their proprietary web-based email applications." *Hately*, 917 F.3d at 790; *see also Lane*, 2016 WL 1271051, at *6 ("Plaintiffs also allege that Defendant accessed electronic files stored on cloud-based servers that were connected to the internet. They further allege that some of the data he accessed consisted of emails. These allegations are sufficient to trigger the SCA.") (citations omitted).

Regardless, determining whether a company is an electronic communication services provider under the Stored Communications Act is typically a factual question for summary judgment or trial. *See Pascal Pour Elle, Ltd. v. Jin*, 75 F. Supp. 3d 782, 788 (N.D. Ill. 2014) ("The Court questions whether Plaintiff will ultimately be able to establish that the Rosy Salon website truly acts as an email or text message provider as intended by the SCA. However, that is a question more appropriately left for summary judgment or trial.").

The Stored Communications Act does create exceptions to liability. The Act's prohibition on accessing communications held in electronic storage does not apply to conduct authorized "by the person or entity providing a wire or electronic communications service," or "by a user of that service with respect to a communication of or intended for that user." *See* 18 U.S.C. § 2701(c)(1)–(2).

Under the first exception, "[a]n entity providing such a communication service can therefore access, and prevent authorized access, to that service." *Bolanos v. Ne. Illinois Univ.*, 2017 WL 56632, at *19 (N.D. Ill. 2017). In other words, electronic communication service providers can access the electronic communications without fear of liability.

"Authorization . . . can be given by the entity providing the electronic communications service, which includes a private employer that provides email service to its employees." *Id.* (alteration in original) (quoting *Joseph v. Carnes*, 108 F. Supp. 3d 613, 616 (N.D. Ill. 2015)). The exception applies to "searches by communications service providers." *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2003). Providers are exempt from liability "for accessing electronic communications stored on *their own servers*." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1032 (N.D. Cal. 2014) (emphasis added).

The second exception covers conduct authorized "by a user of that service with respect to a communication of or intended for that user." *See* 18 U.S.C. § 2701(c)(2). Under that exception, "a 'user' of the service can authorize a third party's access to the communication." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002); *see also In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 509 (S.D.N.Y. 2001) (noting that section 2701(c)(2) creates an "exception for access authorized by authors and intended recipients of electronic communications"). The Act defines "user" as "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." *See* 18 U.S.C. § 2510(13)(A)–(B).

ACW claims that Wrobel accessed its documents (including emails) without authorization, and that Ryan exceeded his authorization when accessing documents. *See* Pl.'s Resp., at 7 (Dckt. No. 13); Cplt., at ¶ 67 (Dckt. No. 1) (discussing Wrobel's use of the Atwater email).

Defendants believe that the Stored Communications Act claim should be dismissed because, in their view, the statutory exceptions apply. *See* Defs.' Mtn. to Dismiss, at 4–5 (Dckt. No. 10). That argument is fair game at the motion-to-dismiss stage, if the complaint itself reveals the applicability of the exception. A court "may dismiss a claim based on a statutory exception that appears on the face of the complaint." *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001).

Defendants' argument is a little rough around the edges. Defendants seem to argue that *Ryan's* conduct falls under the exception in section 2701(c)(1), which covers people or entities who provide the wire or electronic communication service. Also, Defendants seem to contend that *Wrobel's* conduct falls under the exception in section 2701(c)(2), which covers users of the service.

The Court begins with whether an exception applies to Ryan. Defendants contend that Ryan, "as ACW's IT professional," had "the responsibility of 'overseeing and administering access to ACW's system to authorized users.'" *See* Defs.' Mtn. to Dismiss, at 4 (Dckt. No. 10) (quoting Cplt., at ¶ 32 (Dckt. No. 1)). Given his role as IT director, Ryan "was in control of not only setting up and providing ACW's facility, but he was also responsible for determining who was to be provided access to the facility." *Id.*

So, Defendants seem to argue that Ryan authorized his own access because he was the "person . . . providing a wire or electronic communications service." *See* 18 U.S.C. § 2701(c)(1).

ACW responds that the exception does not apply to Ryan. It contends that "ACW is the entity providing the service (not Ryan as an individual who was hired by the company as an IT consultant)." *See* Pl.'s Resp., at 8 (Dckt. No. 13). So, ACW, not Ryan, would be subject to section 2701(c)(1)'s exception for providers.

The Court agrees that Ryan was not "the person . . . providing a wire or electronic communications service." *See* 18 U.S.C. § 2701(c)(1). ACW was. The dictionary defines "provide" as "to supply or make available (something needed or wanted)."[4]

Here, ACW supplied or made available email – through Microsoft 365 – to its employees. ACW "utilize[d] Microsoft's Office 365 . . . cloud services as part of *its IT infrastructure*." *See* Cplt., at ¶ 31 (Dckt. No. 1) (emphasis added). To provide IT capabilities to ACW employees, ACW hired Ryan as a third-party vendor to manage its IT systems.

ACW, not Ryan, provided ACW employees with email accounts. Ryan was simply doing the company's bidding. It was the company's email all along.

Ryan's argument does not fit within the text of the exception, so the argument goes nowhere. And in any event, the argument would create odd results. The argument would, in effect, exempt IT staff from the reach of the statute. It would be strange if the people with the most responsibility for protecting the IT would have the least culpability for abusing the IT.

If Ryan, as a third-party IT consultant, falls within section 2701(c)(1)'s exception for providers, then Ryan could authorize his own conduct that violated ACW's directives. So, if ACW prohibited Ryan from accessing Employee A's email account, Ryan could override that prohibition simply by accessing Employee A's email. And then Ryan could argue that he was immune because he authorized his own conduct.

Here, ACW, not Ryan, determined who was provided email services. According to the complaint, Ryan had no authority to create an account for a fake employee, Jay Atwater. *See* Cplt., at ¶¶ 64, 67–68 (Dckt. No. 1). So, Ryan's access of Atwater's emails was not authorized by ACW. *See Owen v. Cigna*, 188 F. Supp. 3d 790, 795 (N.D. Ill. 2016) (Lee, J.) (declining to

[4] *See Provide*, Merriam-Webster Online, https://www.merriam-webster.com/dictionary/provide (last visited July 24, 2023).

apply section 2701(c)(1)'s exception because "Defendant was not authorized to access [Plaintiff's] att.net email account (at least according to [Plaintiff]), and the resolution of this issue . . . is best reserved for consideration after discovery").

Simply put, the exception does not apply to a rogue contractor. Because Ryan was not the person providing ACW's email services, he is not exempt from liability under the Stored Communications Act.

Next, the Court turns to whether the exception for conduct authorized by the user of an electronic communications service applies to Wrobel. Defendants contend that Wrobel's access falls under the exception in section 2701(c)(2). *See* Defs.' Reply, at 5–6 (Dckt. No. 14). That provision carves an exception for "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user." *See* 18 U.S.C. § 2701(c)(2).

Again, the argument is not exactly clear, but Defendants seem to argue that Ryan was a "user" of ACW's system, and so could authorize Wrobel's access, at least "with respect to a communication of or intended for" Ryan. *See* 18 U.S.C. § 2701(c)(2). Defendants believe that "Wrobel was authorized by the provider to use the service." *See* Defs.' Reply, at 6.

Ryan could not authorize Wrobel's unlimited access under section 2701(c)(2) because at least some of the communications that Wrobel accessed were not "of or intended for" Ryan. *See* 18 U.S.C. § 2701(c)(2). Ryan's ability to grant Wrobel access under the exception is not limitless. At most, the exception covers Wrobel's access to communications that Ryan "author[ed]," or communications where Ryan was the "intended recipient[]." *Goodman v. Goodman*, 2022 WL 17826390, at *18 (S.D.N.Y. 2022).

Here, Ryan gave Wrobel access to ACW's entire system. *See* Cplt., at ¶ 70 (Dckt. No. 1). Using that access, Wrobel viewed documents on ACW's SharePoint system. *Id.* at ¶ 73. But it is not clear from the complaint whether Ryan authored any of these documents or was the intended recipient.

For example, the complaint alleges that in July and August 2022, Wrobel accessed ACW's documents related to risk management and product inventory. *Id.* Based on Ryan's role as an IT consultant, it seems unlikely that Ryan created these documents or that they were "intended for" him. *See* 18 U.S.C. § 2701(c)(2).

At the very least, that question is reserved for a later day. Whether the exception applies is not apparent on the face of ACW's complaint, so the exception is not a basis for dismissal. *See In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d at 507.

Section 2701(c)(2) does not apply to Wrobel's access for another reason. Ryan did not exactly authorize Wrobel to view certain communications on ACW's system. Instead, Ryan was instructed to eliminate Wrobel's access to ACW's systems after Wrobel was fired. *See* Cplt., at ¶ 19 (Dckt. No. 1). But Ryan "disregarded this instruction" and left Wrobel with access to the system. *Id.* So, Ryan didn't give Wrobel the green light – he simply failed to pull the plug.

Maybe Defendants will be able to establish the existence of the exception at summary judgment or trial. But at this stage of the litigation, ACW has plausibly alleged that Wrobel accessed its electronic communications service without authorization.

In sum, the Court denies Defendants' motion to dismiss ACW's claim under the Stored Communications Act.

III. Conversion (Count VI) and Civil Conspiracy (Count VII) Claims

Finally, Defendants move to dismiss ACW's claims for conversion (Count VI) and civil conspiracy (Count VII) under Illinois law. They argue that both state law claims are barred by the economic loss doctrine. *See* Defs.' Mtn. to Dismiss, at 5 (Dckt. No. 10). In Defendants' view, "Plaintiffs' claims for conversion and civil conspiracy seek redress for the same economic harm resulting from the same set of common facts" that supports their breach-of-contract claims against Defendants. *Id.*

Decades ago, the Illinois Supreme Court held that plaintiffs cannot recover for a "solely economic loss" in a tort action. *See Moorman Mfg. Co. v. Nat'l Tank Co.*, 435 N.E.2d 443, 449–50 (Ill. 1982). "Known as the *Moorman* doctrine in Illinois, this doctrine bars recovery in tort for purely economic losses arising out of a failure to perform contractual obligations." *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 567 (7th Cir. 2012).

"The *Moorman* holding is bottomed upon the theory that tort law affords a remedy for losses occasioned by personal injuries or damage to one's property, but contract law and the Uniform Commercial Code offer the appropriate remedy for economic losses occasioned by diminished commercial expectations not coupled with injury to person or property." *In re Illinois Bell Switching Station Litig.*, 641 N.E.2d 440, 444 (Ill. 1994). "*Moorman* dictates that, when a contract sets out the duties between the parties, recovery should be limited to contract damages, even though recovery in tort would otherwise be available under the common law." *R.J. O'Brien & Assocs., Inc. v. Forman*, 298 F.3d 653, 657 (7th Cir. 2002).

The *Moorman* doctrine is not without its limits. Illinois courts recognize three exceptions to the *Moorman* doctrine: "(1) where the plaintiff sustained damage, *i.e.*, personal injury or property damage, resulting from a sudden or dangerous occurrence; (2) where the plaintiff's damages are proximately caused by a defendant's intentional, false representation, *i.e.*, fraud; and (3) where the plaintiff's damages are proximately caused by a negligent misrepresentation by a defendant in the business of supplying information for the guidance of others in their business transactions." *Catalan v. GMAC Mortg. Corp.*, 629 F.3d 676, 693 (7th Cir. 2011).

All three "exceptions have in common an extra-contractual duty between the parties, giving rise to a cause of action in tort separate from one based on the contract itself." *Id.* "Where a duty arises outside of the contract, the economic loss doctrine does not prohibit recovery in tort for the negligent breach of that duty." *Congregation of the Passion v. Touche Ross & Co.*, 636 N.E.2d 503, 514 (Ill. 1994). "Put another way, if a plaintiff claims that a defendant breached an obligation other than a contractual obligation, the *Moorman* doctrine does not apply." *Toll Processing Servs., LLC v. Kastalon, Inc.*, 880 F.3d 820, 827 (7th Cir. 2018) (quotation marks omitted).

For example, if "an architect bungles a construction design, the *Moorman* doctrine bars the aggrieved owner's suit for negligence." *Wigod*, 673 F.3d at 568. "The shoddy workmanship is a breach of the design contract rather than a failure to observe some independent duty of care owed to the world at large." *Id.*

Here, both Wrobel and Ryan entered into contracts with ACW. *See* Cplt., at ¶¶ 49–52 (Dckt. No. 1). Wrobel had an employment contract, and Ryan had a contract as an independent contractor. And both contracts "had provisions safeguarding ACW's proprietary information." *Id.* at ¶ 49. That is, the contracts contained restrictive covenants covering Wrobel's and Ryan's use of ACW's data and information.

In fact, this case involves a breach-of-contract claim against Ryan. AWC alleges that he "was contractually required to maintain the confidentiality of all proprietary information and to not use any proprietary information learned while working at ACW for personal gain or the gain of others." *Id.* at ¶ 141. ACW also brought a breach-of-contract claim against Wrobel that proceeded to arbitration (and is not before the Court). *Id.* at ¶ 21.

Under Ryan's contract, he agreed that he would "not at any time or in any manner, either directly or indirectly, use for [his personal benefit], or divulge, disclose, or communicate in any manner any Confidential Information." *Id.* at ¶ 52. Similarly, Wrobel agreed that he would "not at any time or in any manner, directly or indirectly, use or disclose to any party other than the Company any trade secrets or other Confidential Information." *Id.* at ¶ 50.

So, the question is whether the *Moorman* doctrine bars ACW's claims for conversion and civil conspiracy. The Court holds that it does.

A. Conversion (Count VI)

"To state a claim for conversion under Illinois law, a plaintiff must allege: '(1) an unauthorized and wrongful assumption of control, dominion, or ownership by defendant over plaintiff's personalty; (2) plaintiff's right in the property; (3) plaintiff's right to the immediate possession of the property, absolutely and unconditionally; and (4) a demand for possession of the property.'" *Toll Processing Servs.*, 880 F.3d at 824 (quoting *Gen. Motors Corp. v. Douglass*, 565 N.E.2d 93, 96–97 (Ill. App. Ct. 1990)).

The Seventh Circuit has considered the *Moorman* doctrine in the context of a conversion claim. Basically, the applicability of the doctrine depends on the source of the duty.

If a defendant breached "a common-law duty . . . that arose from a source other than the contract, [then] the *Moorman* doctrine would not bar" the claim for conversion. *Toll Processing Servs.*, 880 F.3d at 827. That is, "[a] conversion claim may not proceed where the duty to the plaintiff arises from the contract." *Kravetz v. Bridge to Life*, 2017 WL 4074016, at *3 (N.D. Ill. 2017). But if "the contract did not contemplate the situation in which the conversion arose," then the *Moorman* doctrine would not stand in the way of the conversion claim. *Id.*

So, whether the *Moorman* doctrine applies to conversion claims depends on the alleged facts, and the nature of the claim at issue. The *Moorman* doctrine bars conversion claims when the defendant allegedly breached a duty created by the contract. *See Meadoworks, LLC v. Linear Mold & Eng'g, LLC*, 2020 WL 4194211, at *4 (N.D. Ill. 2020); *St. George Invs. LLC v. QuamTel, Inc.*, 2014 WL 812157, at *9 (N.D. Ill. 2014) (Dow, J.) (collecting cases); *Kravetz*, 2017 WL 4074016, at *3–4; *Zahran v. Republic Bank of Chicago*, 2019 WL 2583024, at *9 (Ill. App. Ct. 2019) ("Finally, as Republic notes, the parties' relationship was contractual (i.e., it was based on the note) and, therefore, the propriety of the assessment of attorney fees and costs in the payoff of the note is properly determined under the note's terms, not a conversion action, which is a tort claim."); *see also Taizhou Yuanda Inv. Grp. Co. v. Z Outdoor Living, LLC*, 44 F.4th 629, 634 (7th Cir. 2022) (applying Wisconsin's economic loss doctrine to bar a conversion claim).

Other courts have held that the *Moorman* doctrine does not bar conversion claims when the defendant's "conduct violated a duty that was wholly independent of the contract." *Dyson, Inc. v. Syncreon Tech. (Am.), Inc.*, 2019 WL 3037075, at *6–7 (N.D. Ill. 2019).

Here, ACW's conversion claim is about conduct that was covered by its agreements with Ryan and Wrobel. The contracts gave rise to the duty.

Start with Ryan. ACW brings a breach-of-contract claim against him (which Defendants have not moved to dismiss) alleging that he breached his contract by "using and disclosing ACW's trade secrets and confidential information." *See* Cplt., at ¶ 141 (Dckt. No. 1). Ryan "downloaded ACW's proprietary information and then began engaging in activities to compete with ACW" including "by using and disclosing ACW's trade secrets and confidential information." *Id.* at ¶ 143.

ACW's conversion claim incorporates these breach-of-contract allegations by reference. *Id.* at ¶ 146. And it alleges that Ryan violated state tort law for the same reasons that he breached the contractor agreement. "Ryan wrongfully and without authorization assumed control, dominion, or ownership of ACW's data and information that contains ACW's confidential information and trade secrets." *Id.* at ¶ 150.

This alleged conduct is far from "wholly independent of the contract." *Dyson, Inc.*, 2019 WL 3037075, at *7. In fact, Ryan's conduct was "wrongful[]" and "without authorization" in part *because* his contractor agreement with ACW prohibited him from using ACW's data and information in this way. *See* Cplt., at ¶ 150 (Dckt. No. 1).

The same is true of Wrobel's employment contract. Again, the dispute between ACW and Wrobel about the employment agreement went to arbitration, so it is not a claim in the case at hand. Even so, the employment agreement did give rise to the duty. Wrobel's employment contract prohibited him from using or disclosing trade secrets or confidential information. *Id.* at ¶ 50.

ACW's conversion allegations against Wrobel are the same as the allegations against Ryan. ACW alleges that Wrobel "wrongfully and without authorization assumed control, dominion, or ownership of ACW's data and information that contains ACW's confidential information and trade secrets." *Id.* at ¶ 150.

Like Ryan's contract, Wrobel's employment contract covers the conduct at issue in ACW's conversion claim. So, the conversion claim is barred by the *Moorman* doctrine.

ACW argues that its conversion claim survives because "the economic loss doctrine does not bar tort claims when . . . extracontractual duties exist." *See* Pl.'s Resp., at 11 (Dckt. No. 13). That's true, as far as it goes. *See Toll Processing Servs.*, 880 F.3d at 827. But ACW does not explain why the allegations supporting its conversion claim do not flow from a duty under its contracts with Defendants.

True, there is a common-law duty not to convert another's property. *See In re Karavidas*, 999 N.E.2d 296, 309 (Ill. 2013). But here, Ryan's and Wrobel's "contract[s] set[] out the duties between the parties," even if "recovery in tort would otherwise be available under the common law." *R.J. O'Brien & Assocs.*, 298 F.3d at 657. So, by suing in tort over conduct that is covered by the parties' agreements, ACW has brought "a tort claim for purely economic losses arising out of an alleged breach of contract." *Meadoworks*, 2020 WL 4194211, at *4.

ACW also contends that "the Illinois Supreme Court's discussion of the economic loss doctrine has repeatedly recognized that it has no application to intentional torts." *See* Pl.'s Resp., at 11 (Dckt. No. 13). And because "an element of intent exists for claims of conversion," the *Moorman* doctrine does not apply. *Id.* at 12.

The *Moorman* doctrine does not exempt intentional torts. "Although the Illinois Supreme Court has not confronted this precise issue, it has explicitly stated that *Moorman* applies with equal force to cases where a defendant's conduct is negligent and those where, like here, the conduct is alleged to have been intentional." *St. George Invs.*, 2014 WL 812157, at *10 (citing *Morrow v. L.A. Goldschmidt Assocs., Inc.*, 492 N.E.2d 181, 185 (Ill. 1986)). Applying this rule, another court in this district expressly declined "to create an additional broad exception to the doctrine for intentional torts (or at a minimum, the intentional tort of conversion)." *Id.* at *9. This Court also declines to create an exception to the *Moorman* doctrine for intentional torts.

In sum, the *Moorman* doctrine applies to the conversion claims because the underlying duties stemmed from the contractual relationships between ACW and the Defendants.

B. Civil Conspiracy (Count VII)

Defendants also move to dismiss Plaintiff's civil conspiracy claim based on the *Moorman* doctrine. For many of the same reasons given above, the Court dismisses ACW's civil conspiracy claim.

To bring a claim for civil conspiracy, a plaintiff must allege: (1) an agreement between two or more persons for accomplishing either an unlawful purpose or a lawful purpose by unlawful means; and (2) at least one tortious act by one of the co-conspirators in furtherance of the agreement that caused an injury to the plaintiff. *See Borsellino v. Goldman Sachs Grp., Inc.*, 477 F.3d 502, 509 (7th Cir. 2007) (citing Illinois law).

The Illinois Supreme Court recently recognized that civil conspiracy claims may fall under the *Moorman* doctrine's fraud exception. *See Lewis v. Lead Indus. Ass'n*, 178 N.E.3d 1046, 1054–56 (Ill. 2020). But whether the *Moorman* doctrine, or its fraud exception, applies depends on the substance of the allegations supporting the civil conspiracy.

In *Lewis*, the Illinois Supreme Court began by recognizing that civil conspiracy claims can "involve[e] only economic loss," and so may fall under the *Moorman* doctrine. *Id.* at 1054 ("This obviously is a case involving only economic loss, as plaintiffs do not allege any physical injury or property damage and are instead seeking to recover only for the monetary costs of the lead tests."). That is, civil conspiracy claims are not immune from the economic loss doctrine.

The Illinois Supreme Court then reviewed the facts supporting the civil conspiracy and determined that the claim turned on allegations of fraud. *Id.* at 1055. The plaintiffs' civil conspiracy claim "incorporated" by reference the allegations supporting claims for "fraudulent concealment" and "fraudulent misrepresentation." *Id.* So, "plaintiffs' civil conspiracy claim

[was] grounded in the underlying tortious conduct of intentional misrepresentation, *i.e.*, fraud." *Id.*

The *Moorman* doctrine's fraud exception applied because "the conspiracy count here is grounded on a theory of intentional misrepresentation or fraud," so "it falls squarely within that exception to *Moorman*'s prohibition of recovering purely economic loss in tort." *Id.* at 1055. In the fraud context, economic loss, standing alone, is sufficient to avoid the *Moorman* doctrine.

Here, ACW's civil conspiracy claim is not based on fraud. Instead, it alleges a conspiracy "to misappropriate ACW's confidential, proprietary and trade secret information, *and to breach the respective employment agreements* each of [the Defendants] entered into with ACW." *See* Cplt., at ¶ 152 (Dckt. No. 1) (emphasis added). So, ACW's civil conspiracy claim includes a conspiracy to breach the contracts, and the provisions in those contracts prohibiting Defendants from misappropriating "confidential, proprietary and trade secret information." *Id.*

The duty not to breach a contract is not "an extra-contractual duty between the parties." *Catalan*, 629 F.3d at 693 (7th Cir. 2011). The duty stems from the contract itself. So, the alleged duty at the center of ACW's civil conspiracy claim flows from the contract.

The complaint also alleges that "Wrobel led a conspiracy with Ryan to unlawfully access, misappropriate, use and disclose ACW's trade secrets and confidential information." *See* Cplt., at ¶ 154 (Dckt. No. 1). As discussed, these allegations overlap with the alleged breaches of contract. *Id.* at ¶¶ 50, 52. The civil conspiracy allegations here do not allege fraud. Instead, they allege the same facts supporting a breach-of-contract claim.

Finally, for the reasons stated above, the Court rejects ACW's argument that the *Moorman* doctrine does not apply to intentional torts like civil conspiracy. *See St. George Invs.*, 2014 WL 812157, at *9–10.

* * *

In sum, the Court grants the motion to dismiss the conversion and civil conspiracy claims (Counts VI & VII) based on the economic loss doctrine.

Conclusion

For the foregoing reasons, the motion to dismiss is denied in part and granted in part. The Court denies Defendants' motion to dismiss Plaintiff's claims under the Computer Fraud and Abuse Act (Count I) and the Stored Communications Act (Count II). The Court grants Defendants' motion to dismiss Plaintiff's conversion (Count VI) and civil conspiracy (Count VII) claims.

Date: July 26, 2023

Steven C. Seeger
United States District Judge